
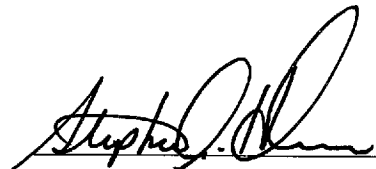


Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number (Optional): 4015-721/P12472-US1	
<p>I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]</p> <p>Date: January 10, 2008</p> <p>Signature: </p> <p>Typed or printed name: KATHLEEN KOPPEN</p>		Application Number: 09/727,062	Filed: November 30, 2000
		First Named Inventor: Dent	
		Art Unit: 2134	Examiner: PETER POLTORAK
<p>Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request</p> <p>This request is being filed with a notice of appeal.</p> <p>The review is requested for the reason(s) stated on the attached sheet(s). Note: No more than five (5) pages may be provided.</p> <div style="display: flex; justify-content: space-between; align-items: flex-start; margin-top: 20px;"><div style="width: 45%;"><p>I am the</p><p><input type="checkbox"/> applicant/inventor</p><p><input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)</p><p><input checked="" type="checkbox"/> attorney or agent of record Registration Number: <u>47,642</u></p><p><input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration Number if acting under 37 CFR 1.34: _____</p></div><div style="width: 50%; text-align: center;"> Signature <u>Stephen A. Herrera</u> Typed or Printed Name <u>(919) 854-1844</u> Telephone Number <u>January 10, 2008</u> Date</div></div> <p>NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.</p> <p><input type="checkbox"/> *Total of _____ form(s) is/are submitted.</p>			

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of
Paul Dent

Serial No.: **09/727,062**

Filed: **November 30, 2000**

For: **Anti-Spoofing Password Protection**

Docket No: **4015-721**

PATENT PENDING

Examiner: Peter Poltorak

Group Art Unit: 2134

Confirmation No.: 2720

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

- ☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
- ☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (571) 273-8200.

January 10, 2008

Date

Kathleen Koppen

This correspondence is being:

- ☒ electronically submitted via EFS-Web

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Sir:

Applicants submit the following remarks in support of the Pre-Appeal Brief Request for Review attached herewith. Claims 1-5, 7-12, 14-15, 17-18, and 20 are currently pending. The Examiner maintains that the independent claims 1 and 11 are obvious over Pichlmaier (U.S. Pat. No. 5,317,637) in view of Windows NT as evidenced by Ozzie (U.S. Pat. No. 5,664,099) and Hadfield ("Windows NT Server 4 Security Handbook," 1997, ISBN: 078971213). However, Pichlmaier does not teach or suggest what the Examiner says it does. Further, those of ordinary skill in the art having common sense at the time the invention was made would never have reasonably considered modifying the references as the Examiner asserts.

Claim 1 relates to a method of performing a password-protected secure function on a computing device. The method prevents a malicious entity from "spoofing" a password entry

screen associated with the secure function and fraudulently obtaining a user's password or other private data. For convenience, claim 1 appears below:

1. A method implemented by a security module in a computing device of performing a password-protected secure function, the method comprising:
 - storing authentication indicia for authenticating password entry screens to a user in a memory of the computing device;
 - receiving a command to execute a password-protected secure function;
 - temporarily halting execution of programs not needed by the security module while the data entry screen is displayed;
 - prompting the user to enter a password associated with the secure function by displaying a password entry screen containing the authentication indicia responsive to receiving the command;
 - removing the data entry screen from the display;
 - restarting halted programs after the password entry screen is removed from the display; and
 - executing the password-protected secure function based on the validity of the password entered by the user.

Claim 1 stores authentication indicia (i.e., a reverse password) in memory. When a user enters a command to execute a secure function, the password entry screen is displayed responsive to receiving a command to execute a secure function, claim 1 authenticates a password entry screen to the user by including the authentication indicia on the password entry screen. Thus, the mere presence or absence of the authentication data on the password entry screen indicates to the user whether that screen is valid or spoofed.

The Examiner admits that Windows NT (i.e., as illustrated by Ozzie and Hadfield) does not teach or suggest storing authentication indicia for authenticating password entry screens to a user, but asserts that Pichlmaier does. *Final Office Action*, p. 4, ¶8. It does not. Pichlmaier discloses communicating an encoded data word over a network to authenticate remotely located computers to a user at a local computer. *Pichlmaier*, col. 2, ll. 17-21. The local computer decodes and displays the data word (e.g., "ROSE") to the user upon successfully completing a validation process. If the data word is accurate, the remote computer is a valid computer, and the user can feel secure about sending any private data, such as a Personal Identification Number (PIN) to that computer. *Pichlmaier*, col. 2, ll. 57-63.

The rejection ignores an important factual difference between the authentication indicia and its function in the claimed invention and Pichlmaier. With the claimed invention, the mere presence or absence of the stored authentication indicia from the password entry screen allows the user to instantly differentiate a valid password entry screen from an invalid or “spoofed” password entry screen. In contrast, the Pichlmaier data word does not perform this function, nor is it intended to perform this function. The data word that Pichlmaier stores is for system validation only. A correctly decoded data word indicates only that the remote computer is a valid computer in the system. It says nothing of a password entry screen – indeed, the entry screen in Pichlmaier appears after the validation process is complete. Thus, while a user may be certain that a remote computer is valid within the system; there is no guarantee that a password entry screen displayed on the local computer is valid and not “spoofed.”

Therefore, Pichlmaier does not teach or suggest, “storing authentication indicia for authenticating password entry screens to a user.” Rather, Pichlmaier encodes/decodes a data word transmitted across a computer network to validate a completely different computer. And the Examiner’s admission regarding the failure of Windows NT to remedy this deficiency means that none of the cited references, alone or in combination, teaches or suggests each and every element of claim 1.

Notwithstanding the above, no one skilled in the art and having common sense at the time the invention was made would reasonably consider modifying the references as the Examiner alleges. The Examiner alleges that it would be obvious to modify both Pichlmaier and Windows NT in view of the other’s teachings. Specifically, that one skilled in the art would be motivated to implement indicia into the Windows NT password entry screen to verify the authenticity of the device system, and to implement Windows NT into a Pichlmaier device to establish a protected channel between the user and a legitimate program. *Final Office Action*, p. 4, ¶18. Both allegations are conclusory and unsupported by the references.

Pichlmaier operates based on a data exchange between computers. To accomplish its intended function, Pichlmaier requires an operating system such as Windows NT, a random number generator application to generate the data word, a communication application to communicate the data word with remotely located computers, and an encoding/decoding application to encode/decode the data word. Each application must be executing for the Pichlmaier authentication process to operate. According to Ozzie, however, Windows NT “terminates any application programs which are in operation during the password entry sequence.” Ozzie, col. 1, ll. 46-66 (emphasis added). Thus, Windows NT could not be modified to implement Pichlmaier because Windows NT is designed to terminate the very same types of application processes that the Pichlmaier authentication process requires to function. This would render Pichlmaier unusable for its intended purpose.

Additionally, Windows NT terminates such application programs to establish a protected channel between the user and a legitimate program (i.e., the login program). That is, Windows NT by itself performs the exact functionality that the Examiner reasons would be the motivation to combine the references. One skilled in the art would never reasonably consider combining two references in the manner suggested by the Examiner to obtain an end-result that one of the references already provides.

The reasons for the rejections are conclusory. The references do not support the Examiner’s allegations as is required by the law. Accordingly, none of the references teaches or suggests, alone or in combination, claim 1 or any of its dependent claims.

Claim 11 also stands rejected as obvious over the same references and for substantially the same reasons as those stated above for claim 1. However, claim 11 is an apparatus claim for carrying out the method of claim 1, and thus, recites similar language.

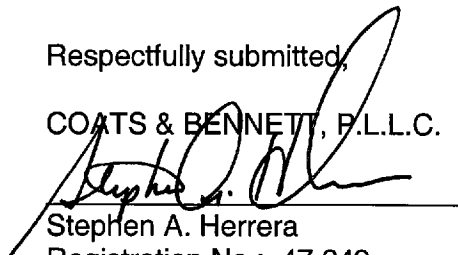
11. A device for executing a password-protected secure function comprising:
a secure processor configured to receive a command to execute a password-protected secure function, and to execute a password program to obtain a password associated with the password-protected secure function from a user responsive to receiving the command;
memory operatively connected to the secure processor and configured to store authentication indicia for authenticating password entry screens to the user of the device;
a display operatively connected to the secure processor; and
the secure processor configured to:
output a data entry screen containing said the authentication indicia to said the display;
temporarily halt execution of programs not needed by the secure processor while the password entry screen is displayed;
remove the data entry screen from the display;
restart halted programs after the password entry screen is removed from the display; and
execute the password-protected secure function based on the validity of the password entered by the user.

For reasons similar to those stated above, none of the references teaches or suggests, alone or in combination, claim 11 or any of its remaining dependent claims.

In conclusion, none of the references, alone or in combination teaches or suggests any of the pending claims. Therefore, the §103 rejections of claims 1 and 11, and of their respective dependent claims, fail and must be withdrawn.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.


Stephen A. Herrera
Registration No.: 47,642
1400 Crescent Green, Suite 300
Cary, NC 27518
Telephone: (919) 854-1844
Facsimile: (919) 854-2084

Dated: January 10, 2008